REMARKS

Claims 2-25 and 28-53 remain in the application. Claims 1, 26 and 27 have been canceled. Claims 2 and 4-12 have been amended and claims 28-53 have been added in order to more clearly define applicant's invention. Claims 13-25, drawn to a non-elected invention, are withdrawn from consideration. Applicants note with appreciation that claims 9-12 are considered allowable if rewritten in independent form. These claims however, have not been rewritten in independent form in the belief that all of the claims are now considered allowable.

Claims 1-12 and 25-27 have been rejected under 35 U.S.C. §112, second paragraph. Claims 1-12 and 26-27 have also been rejected under 35 U.S.C. §103 (a). These rejections are respectfully traversed and reconsideration is requested in view of the foregoing amendments and following remarks.

Claims 1-12 and 25 (sic) -27 have been rejected under 35 U.S.C. §112, second paragraph, because the Examiner believes that these claims are indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is noted that claim 25 is directed to a non-elected invention, and is considered withdrawn. Applicants believe the that it was the intent of the Examiner to reject claims 1-12, 26 and 27, and not claim 25, under 35 U.S.C. § 112, second paragraph. Accordingly, Applicant's comments are directed to the more limited grouping.

The Examiner states that with regard to claim 1, "it is unclear where the query is coming from or who queries to the server and what is being queried." The Examiner also states that "it is unclear how the system is providing a secure domain name service." Claim 1 has been canceled in favor of new claim 28. It is submitted that a query can originate from any source and provided to the domain name service recited in claim 28, with the domain name service configured "to receive a query for a network address." Further, the clarifying amendments presented by new claim 28 should address the second issue raised by the Examiner.

Regarding the rejection of claims 26 and 27, the Examiner states that "it is unclear what kind of apparatus [the claimed subject matter] it is. It is unclear how this apparatus is configured. And, it is unclear for what a computer network address is queried. (sic)" Again, it is submitted that the clarifying amendments presented by new claim 28 should render the rejection moot. Claim 28 specifically describes the configuration of the domain name service system for establishing a secure communication link.

Claims 1-12, 26 and 27 have also been rejected under 35 U.S.C. § 103(a) as being unpatentable over IP Security Chapter 13 of XP-002167283 (also referred to as XP). Claims 1, 26 and 27 have been canceled. It is submitted that the reference neither anticipates nor makes obvious the claimed invention as defined by new claim 28.

New claim 28 recites a system for providing a domain name service for establishing a secure communication link. The system comprises a domain name service system configured to be connected:

to a communication network,

to store a plurality of domain names and corresponding network addresses,

to receive a query for a network address, and

to comprise an indication that the domain name service system supports establishing a secure communication link.

It is submitted that the reference XP neither anticipates nor makes obvious the claimed subject matter of claim 28, and the claims dependent thereon. The Examiner cites pages 399 and 400 of XP. These pages describe prior art approaches to IP security known at the time the reference was published (1998). XP mentions:

> ...security mechanisms in a number of application areas, including electronic mail (S/MIME, PGP), client/server Kerberos), Web access (Secure Sockets Layer), and others. However, users have some security concerns that cut across protocol layers. For example, an enterprise can run a secure, private TCP/IP network by disallowing links to untrusted sites, encrypting packets that leave the premises, and authenticating packets that enter the premises. By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but for the many security-ignorant applications.
>
> IP-level security encompasses three functional areas: authentication, confidentiality, and key management. The authentication mechanism

> assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet has not been altered in transit. The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties. The key management facility is concerned with the secure exchange of keys...

Thus, the reference describes the three function areas of any security system for protecting transmitted data across any network. The reference goes on to cite a 1994 report of the Internet Architecture Board that states that the Internet needs more and better security, and it identifies key areas for security mechanisms. Among these are the need to secure the network infrastructure form unauthorized monitoring and control of network traffic and the need to secure end-user-to-end-user traffic using authentication and encryption mechanisms. The report cites reported security incidents, the most serious types of attacks including IP spoofing, and various forms of eavesdropping and packet sniffing. Thus, the reference generally describes the need for secure transmission of data.

In describing IP Security (IPSec) the reference goes on to state:

> IPSec provides the capability to secure communications across a LAN, across private and public wide area networks (WANs), and across the Internet. Examples of its use include the following:
>
> Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
>
> Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters...

The reference states at the bottom of page 400, "the principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level."

The reference describes the overall architecture in Figure 13.2 (page 403). The blocks shown in the Figure are defined on pages 403 and 404. It is clear that the

architecture described and shown in the reference does not describe nor even suggest a domain name service system configured to be connected to a communication network, to store a plurality of domain names and corresponding network addresses, to receive a query for a network address, and to comprise an indication that the domain name service system supports establishing a secure communication link. (cf., claim 28 of the above-identified application).

Dependent claims 2-12 and 29-51 currently under consideration in the application are dependent from independent Claim 28 discussed above and therefore are believed to be allowable over the applied reference for at least the same reasons. Because each dependent claim is deemed to define an additional aspect of the invention, the individual consideration of each on its own merits is respectfully requested.

Finally, claims 52 and 53 have been added. Claim 52 recites "a machine-readable medium comprising instructions executable in a domain name service system. The instructions comprise code for connecting the domain name service system to a communication network; storing a plurality of domain names and corresponding network addresses; receiving a query for a network address; and supporting an indication that the domain name service system supports establishing a secure communication link." Claim 53 recites "a method of providing a domain name service for establishing a secure communication link. The method comprises connecting a domain name service system to a communication network, the domain name service system comprising an indication that the domain name service system supports establishing a secure communication link; storing a plurality of domain names and corresponding network addresses; and receiving a query for a network address for communication."

Accordingly, all of the pending claims currently under consideration, claims 2-25 and 28-53, are believed to be patentable over the cited reference. An early and favorable action thereon is therefore earnestly solicited.

If a telephone conference will expedite prosecution of the application, the Examiner is invited to telephone the undersigned.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: 11 July 2007

Toby H. Kusmer, P.C.
Reg. No. 26,418
Attorney for Applicants
28 State Street
Boston, MA 02109-1775
DD Telephone: (617) 535-4065
Facsimile: (617)535-3800
e-mail: tkusmer@mwe.com